In the Claims:

- (Currently Amended) A <u>client-based</u> method, comprising:
 obtaining a hint;
 obtaining a password;
 performing a hashing algorithm on the hint and the password to generate a key;
 encrypting data using the key; and
 sending the encrypted data to a server for storage.
- 2. (Original) The method of claim 1, wherein the step of performing a hashing algorithm includes hashing the password.
- 3. (Original) The method of claim 1,
 wherein the step of performing a hashing algorithm includes hashing the
 password to derive a first secret, hashing the first secret to derive a second secret, hashing
 the hint and the first secret to generate an intermediate index, and hashing the
 intermediate index and the second secret to generate the key.

 α^{1}

- 4. (Currently Amended) A <u>client</u> system, comprising:
 - a user interface for obtaining a password;
- a key generator coupled to the user interface for performing a hashing algorithm on a hint and the password to generate a key;
- an encryption engine coupled to the key generator for encrypting data using the key; and
- a communications module coupled to the engine for sending the encrypted data to a server for storage.
- 5. (Original) The system of claim 4, further comprising a hint generator for generating the hint.
- 6. (Original) The system of claim 4, wherein the key generator hashes the password.

- 7. (Original) The system of claim 4, wherein the key generator hashes the password to derive a first secret, hashes the first secret to derive a second secret, hashes the hint and the first secret to generate an intermediate index, and hashes the intermediate index and the second secret to generate the key.
- 8. (Currently Amended) A <u>client</u> system, comprising:

means for obtaining a hint;

means for obtaining a password;

means for performing a hashing algorithm on the hint and the password to generate a key;

means for encrypting data using the key; and means for sending the encrypted data to a server for storage.

- 9. (Original) The system of claim 8, wherein the system includes code stored on a computer-readable storage medium.
- 10. (Original) The system of claim 8, wherein the system includes code embodied in a carrier wave.
- 11. (Original) A method, comprising:

receiving a request to store encrypted data from a client;

sending an encryption downloadable for deriving a key to encrypt data to the client;

receiving encrypted data that was encrypted by the encryption downloadable from the client; and

obtaining a hint, corresponding to the encrypted data and needed for regenerating the key; and

3

storing the hint and the encrypted data.

PaloAlto/61610.1

12. (Original) A system, comprising:

an encryption downloadable for deriving an encryption key from a password and a hint;

a web server for interfacing with a client, for sending the encryption downloadable to the client, and for receiving encrypted data that was encrypted by the encryption downloadable from the client; and

memory coupled to the web server for storing a hint corresponding to the encrypted data and needed to regenerate the key from the client and the encrypted data.

13. (Currently Amended) A <u>client-based</u> method, comprising:

obtaining a password;

receiving encrypted data and a hint corresponding to the encrypted data from a server; and

performing a hashing algorithm on the password and the hint to generate a key for decrypting the encrypted data.

14. (Original) The method of claim 13, wherein the step of performing a hashing algorithm includes hashing the password.

15. (Currently Amended) A <u>client</u> system, comprising:

a user interface for obtaining a password;

a communications module for receiving the encrypted data and a hint corresponding to the encrypted data from a server;

a key generator for performing a hashing algorithm on the password and the hint to generate a key for decrypting the encrypted data.



16. (Currently Amended) A <u>client</u> system, comprising: means for obtaining a password;

means for receiving encrypted data and a hint corresponding to the encrypted data from a server; and

means for performing a hashing algorithm on the password and the hint to generate a key for decrypting the encrypted data.

- 17. (Original) The system of claim 16, wherein the system includes code stored on a computer-readable storage medium.
- 18. (Original) The system of claim 16, wherein the system includes code embodied in a carrier wave.

0,

19. (Original) A method, comprising:

receiving identification of encrypted data;

sending a decryption downloadable for deriving a key from a password and a hint to a client; and

sending a hint corresponding to the encrypted data to the client.

20. (Original) A system, comprising:

a decryption downloadable for deriving a key from a password and a hint; encrypted data;

a hint corresponding to the encrypted data; and

a web server for interfacing with a client, and for sending the decryption downloadable, the encrypted data and the hint to the client.

- 21. (Original) A client-based method, comprising: obtaining a password; deriving a first secret from the password; receiving a hint corresponding to data to be decrypted from a server; deriving an intermediate index from the first secret and the hint; and sending the intermediate index to the server.
- 22. (Original) The method of claim 21, wherein deriving the first secret includes hashing the password.
- 23. (Original) The method of claim 21, wherein deriving an intermediate index includes hashing the first secret and the hint.
- a user interface for obtaining a password;
 an index generator coupled to the user interface for generating an intermediate index from a hint received from a server and a secret derived from the password; and a communications engine coupled to the index generator for sending the intermediate index to the server.
- 25. (Original) The system of claim 24, wherein the index generator generate the intermediate index by hashing the hint and the secret.
- 26. (Original) A system, comprising: means for obtaining a password; means for deriving a first secret from the password; means for receiving a hint corresponding to data to be decrypted from a server; means for deriving an intermediate index from the first secret and the hint; and means for sending the intermediate index to the server.

 \mathcal{N}

24.

(Original) A system, comprising:

- 27. (Original) The system of claim 26, wherein the system includes code stored on a computer-readable storage medium.
- 28. (Original) The system of claim 26, wherein the system includes code embodied in a carrier wave.
- 29. (Original) A server-based method, comprising:receiving an indication of encrypted data to be decrypted;

transmitting to a client a hint corresponding to the indication, and a decryption downloadable for deriving an intermediate index from a password and the hint;

receiving the intermediate index from the client; and

deriving a decryption key from a second secret corresponding to the user and the intermediate index.

30. (Original) A system, comprising:

a second secret corresponding to a user;

a decryption downloadable for generating an intermediate index from a password and a hint;

a web server for receiving an indication of encrypted data to be decrypted, for transmitting the decryption downloadable and a hint corresponding to the indication to a client, and for receiving an intermediate index from the client; and

a server-resident module for deriving a key for decrypting the encrypted data from the second secret and the intermediate index.

W